AMC Regulation 25-75

Information Management:

U.S. Army Materiel Command (AMC) Web Management Program

U.S. Army Materiel Command
9301 Chapek Road
Fort Belvoir, VA 22060-5527
23 JULY 2004

UNCLASSIFIED

DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
9301 CHAPEK ROAD, FORT BELVOIR, VIRGINIA 22060-5527

AMC REGULATION NO. 25-75 — 23 July 2004

U.S. ARMY MATERIEL COMMAND (AMC) WEB MANAGEMENT PROGRAM

1. Purpose. To establish policy, guidance, responsibilities, and procedures for the Army Materiel Command AMC Web Management program in accordance with Federal, DoD and Army policy and guidance.

2. Applicability. This regulation applies to all AMC organizations and activities with public and restricted websites and web applications, including all personnel (military, Government civilian, and contractors/consultants) who create, operate, or maintain AMC websites.

3. Scope. The guidance prescribed herein governs the development, deployment, operation, and governance of all AMC public and restricted websites whether developed and deployed by AMC webmasters, contract support staff or other support personnel authorized to develop and/or maintain websites or web applications.

---

*This regulation supercedes Policy Memorandum # 03-01, 14 Dec 2001.

4. Explanation of Terms and Abbreviations.

a. Website: any static or dynamic application that is accessed by a browser.

b. Webified System/web application: any application where the end-user accesses information via a Web browser.

c. 508 compliant: A website or web application that meets the terms and conditions of Section 508.

d. Proponent: Commander, Director, Office Chief or Activity Chief of an AMC element responsible for a particular website.

e. Sections 501, 504 and 508 of the Rehabilitation Act: Section 501 prohibits discrimination on the basis of disability in Federal employment, and requires federal agencies to provide for reasonable accommodation in the workplace. Section 504 provides for general nondiscrimination, and applies to federal programs, services and activities. Section 508 is a part of the Rehabilitation Act of 1973 which requires that electronic and information technology developed, procured, maintained, or used by the Federal government be accessible to people with disabilities. Section 501 and 504 are referenced since they are directly tied to Section 508 to ensure accessibility.

g. AR 25-2: A regulation that establishes policies and assigns responsibilities for all users and developers for achieving acceptable levels of Information Assurance (IA) in the engineering, implementation, operation, and maintenance (EIO&M) for all Information Systems (IS) across the U.S. Army Enterprise Infostructure (AEI).

h. FOUO: For Official Use Only. This information may be disseminated within DoD Components and between officials of DoD Components and DoD contractors, consultants, and grantees to conduct official business for the Department of Defense.

i. Department of Defense Freedom of Information Act (FOIA) Guidance: This includes guidance for the Removal of Personally Identifying Information of DoD Personnel from Unclassified websites.

j. OPSEC: Operations Security.

5. Policy.

a. The Web Management Program, a support element of the HQ AMC Command Strategy, is a collaborative effort between the AMC Chief Information Office (AMC CIO/G-6), AMC Major Subordinate Commands (MSCs) and Separate Reporting Activities (SRAs). It is the official HQ AMC mechanism that addresses consistency among AMC websites. In addition, the Web Management Program serves to establish a standard operating procedure for AMC webmasters that includes consistent web design compatible with industry best practices and is compliant with all federal requirements and mandates that apply to DoD Websites, including, but not

limited to, sections 501, 504 and 508 of the Rehabilitation Act; FOUO, FOIA and (OPSEC) guidance.

The components of the web management program will consist of the following:

1. Quarterly Compliance Testing.
2. Resources for web management.
3. Detailed Processes and Procedures to ensure compliance, for the conduct of the Web Management Program (please refer to para. 7).
4. Inventory of all AMC websites and web applications.
5. The establishment of a web management working group.

b. The Web Management Program grants authority to the AMC CIO/G-6 to monitor websites and web applications for compliance. The AMC CIO/G-6 will conduct systematic reviews of all public and restricted Websites and web applications to assess compliance with this document.

c. AMC websites and web applications, as defined herein, must adhere to all applicable Federal, DoD, Army and AMC mandates. A page for easy reference with links to the applicable mandates will be provided on an AMC webmaster web site located on Army Knowledge Online (AKO), the Army's Enterprise portal.

d. Web developers must design websites and web applications that meet the needs of all users who require access to AMC information to include individuals with disabilities. Industry "Usability Guideline" considerations will also be addressed in the design of websites and web applications and the usability standards will be included wherever possible and feasible.

e. AMC CIO/G-6 must ensure that the procurement of web services takes into account the needs of all end users - including people with disabilities. Websites and web applications must also adhere to all applicable DoD, DA and Federal guidelines. Websites and web applications found to be in violation of Sections 501, 504, 508, FOUO, FOIA, OPSEC, and AR 25-2 will be addressed on a case-by-case basis. Websites and web applications not in compliance will be placed on a Noncompliance List. The web site/web application proponent will provide a plan and projected date for achieving compliance to the AMC CIO/G-6. The Noncompliance List will be reviewed for progress towards compliance on a quarterly basis. If it is not possible for the site/application to be made compliant, it will be necessary for the proponent organization to provide justification to receive approval from the AMC CIO/G-6 for continued operation.

f. The provisions of Sections 501, 504, 508 will be followed if non-compliance presents an "undue burden." The affected organization must produce a recovery plan in response to the undue burden provisions. If the plan for compliance is not met, the website or web application may be placed offline, and not be allowed to operate until compliance is achieved. All exceptions will have to be managed on an individual basis. The compliance status on individual websites/applications will be sent to the appropriate parties via encrypted email. The provisions of FOUO, FOIA, OPSEC, and AR 25-2 must be followed at all times.

g. Websites must comply with the applicable requirements of AR 25-2, Information Assurance, as well as with FOUO, FOIA, and OPSEC.

h. Evaluations will be conducted at each AMC organization that owns a public/private website(s). The evaluations will be performed on a quarterly basis; however, evaluations may be made of any AMC website or web application when circumstances dictate. Guidance is currently being developed to address the evaluation and testing processes and procedures.

i. The result of the evaluations will be summarized and provided to the AMC CIO/G-6 and to the proponent organization's webmaster.

6. Responsibilities. The following responsibilities are assigned for the management of the AMC Web Management Program:

a. AMC CIO/G-6 - As the authority for the AMC Web Management Program the AMC CIO/G-6 will take all necessary actions to ensure AMC websites and web applications comply with appropriate directives. Specifically, the CIO will:

(1) Establish and maintain an inventory of all AMC websites and web applications.

(2) Conduct random compliance evaluations of AMC's websites and web applications.

(3) Submit a consolidated compliance report to the AMC Command Group.

(4) Provide guidance and direction in the establishment of websites and web applications.

(5) Function as the AMC Section 508 and Web Management point of contact.

(6) Manage and respond to all higher Headquarters' tasking and information requests.

b. Website and web application proponents - Each website/web application proponent is responsible for compliance of their Websites with appropriate directives, including this regulation. Specifically, proponents will:

(1) Register all websites and web applications with the AMC CIO/G-6.

(2) Submit "self-compliance" reports to the AMC CIO/G-6.

(4) Notify the AMC CIO/G-6 of the requirement for a Web site or and Web application prior to development.

(5) Ensure proposed Websites and web applications meet mission requirements and are not duplicative of other AMC Websites.

(6) Submit quarterly compliance reports to the AMC CIO/G-6.

7. Implementing Procedures. The CIO will develop and promulgate detailed procedures for the conduct of the Web Management Program. In the interim, the following procedures are in effect immediately:

a. The AMC CIO will:

(1) Establish and maintain an inventory and prescribe procedures for registration of all AMC websites and web applications into the AMC Webmaster Registry.

(2) Conduct random compliance evaluations of AMC's websites and web applications.

(3) Submit a consolidated compliance report to the command group and to the organization CIO and webmaster.

b. Website/Web application proponents will:

(1) Ensure that each deployed website and web application is compliant with the requirements stated herein.

(2) Register all public and restricted, websites and web applications on the AMC Web Management Program website located at http://137.80.5.31/section_508/. Additionally, register all public Websites and web applications in the DoD GILS registration system located at: https://sites.defenselink.mil/.

(3) Ensure each private/public website is reachable via a link on their organization's AKO Community page. Detailed processes and procedures will be published separately.

(4) Ensure that all websites and web applications have an FOIA-compliant email address and phone number (including area code and DSN) posted on the site/application. This will enable users to notify the designated party of any problems or questions on the site/application

(5) Ensure that each deployed website and web application is compliant with the OPSEC requirements (see Appendix B).

(6) Conduct periodic compliance testing.

(7) Comply with the reporting requirements established in this regulation.

(8) Ensure that all websites and web applications have a 'Date of Last Update' displayed on at least the "home page." Link the 'Date of Last Update' to a 'Change Log' that describes in summary form the changes made in reverse chronological order (most current first). This action will expedite the validation process by the AMC CIO and proponent by providing a standardized configuration management process for changes.

(9) Not use "Under Construction" pages or notices.

(10) Ensure that each website or web application has a written security plan to document needed security access levels required.

(11) Ensure that each website and web application that requires Secured Sockets Layer (SSL) is registered with the appropriate Public Key Interface (PKI) provider.

(12) Ensure all websites/applications comply with the requirements of AR 25-2.

(13) Ensure all websites/applications comply with FOIA guidance.

(14) Ensure all websites/applications comply with FOUO guidance.

(15) Ensure all websites/applications comply with OPSEC guidance.

(16) Ensure all "private" websites employ login and password.

The proponent of this regulation is the Chief Information Officer/G-6, U.S. Army Materiel Command. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, HQ AMC, ATTN: AMCIO-SPO, 9301 Chapek Road, Fort Belvoir, VA 22060-5527

FOR THE COMMANDER:

//signed//
RICHARD A. HACK
Lieutenant General, USA
Deputy Commanding General

APPENDIX A
References

a. Federal

Electronic and Information Technology Accessibility Standards, Architectural and Transportation Barriers Compliance Board, Federal Register, December 21, 2000, 36 CFR Part 1194 (Section 508).
http://www.access-board.gov/sec508/508standards.htm

Federal Acquisition Regulation: Electronic and Information Technology Accessibility, Federal Register, Apr 25, 2001, 48 CFR Parts 2, 7, 10, 11, 12, and 39.
http://www.ogc.doc.gov/ogc/contracts/cld/facs/fac97-27.pdf

US Access Board, Electronic and Information Technology Accessibility Standards, Economic Assessment, November 2000.
http://www.access-board.gov/sec508/assessment.htm

Workforce Investment Act of 1998.
http://www.usdoj.gov/crt/508/508law.html

Section 501, Rehabilitation Act of 1973.
http://www.eeoc.gov/policy/rehab.html

Section 504, Rehabilitation Act of 1973.
http://www.eeoc.gov/policy/rehab.html

b. US Government

Privacy Act (5 U.S.C. 552a)
http://www.usdoj.gov/foia/privstat.htm

Computer Security Act of 1987 (40 U.S.C. 759 note)
http://www.ssa.gov/OP_Home/comp2/F100-235.html

Public Law 100-235, Computer Security Act of 1987
http://www.amc.army.mil/amc/ci/matrix/documents/public_law/pl_100-235.pdf

Copyright Act of 1976 (Title 17, United States Code, Section 101-810.) and Copyright Basics, Circular 1, Copyright Office, Library of Congress, Washington, DC, January 1991
http://www.copyright.gov/title17/circ92.pdf

Federal Records Act (44 U.S.C. Chapters 29, 31, 33, 35), National Archives and Records Administration Regulations (36 CFR Chapter 12, Subchapter B, "records Management")
http://www.ojp.usdoj.gov/oa/fedwebguide/statues.htm

Establishment of Government Information Locator Service, OMB Bulletin No. 95-01
OMB Circular A-130, "Management of Federal Information Resources"
http://www.whitehouse.gov/omb/bulletins/95-01.html

Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35), 61 CFR 6428 (February 20, 1996)
http://www.archives.gov/federal_register/public_laws/acts.html#pra

Freedom of Information Act (FOIA)
http://www.defenselink.mil/pubs/foi/

c. DoD

Memorandum, Deputy Secretary of Defense, 7 February 1995, subject: Clearance Procedures for Making Electronic Information Available to the Public (enclosure 1)

Memorandum, SA/CSA 8 August 2001, Army Knowledge Management Guidance Memorandum Number 1

Department of Defense (DoD) Web Site Administration Policies and Procedures 25 November 1998 (amended April/26/2001) - Includes Cookie Policy

DoD Directive 5230.9, Clearance of DoD Information for Public Release

DoD Instruction 5230.29, Security and Policy Review of DoD Information for Public Release

DoD Directive 5120.4 amended, Electronic Newspaper Policy

DoD 5500.7-R, change 2, Joint Ethics Regulation (JER), 25 Mar 1996

For Official Use Only (FOUO)
http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html
(Note: Questions about FOUO should be directed to your local FOIA Office. Questions about aggregated information should be referred to your local security office and/or OPSEC coordinator)

Freedom of Information Act (FOI|A) Guidance
http://www.defenselink.mil/pubs/foi/guidance.html

DoD Directive 5015.2, Records Management

Domain Registration in the .mil Domain

Mobile Code Memorandum 7 Nov 2000

d. Army

Guidance for Management of Publicly Accessible U.S. Army Websites, 30 November 1998

AR 25-1, The Army Information Resource Management Program, http://www.army.mil/webmasters/AR25-1.doc

AR 25-55, The Department of the Army Freedom of Information Act Program, 10 January 1990 (update)

AR 340-21, Office Management, The Army Privacy Program, 5 July 1985

AR 360-5, Public Information, 31 May 1989

AR 380-5, Department of the Army Information Security, 1 August 1990

AR 380-19, Security, Information Systems Security, 1 August 1990

AR 530-1, Operations and Signal Security, Operations Security (OPSEC), 15 October 1985

TWX, R 081630Z Mar 95, SAIS-ZA, Director of Information Systems, Command, Control, Communications, and Computers, subject: The Army Presence on the INTERNET World Wide Web

TWX, P 051348Z Feb 96, SAIS-ZA, Director of Information Systems, Command, Control, Communications, and Computers, Password Protection for the World Wide Web Home-pages

Information Assurance
http://www.army.mil/usapa/epubs/pdf/r25_2.pdf

e. AMC

http://www.amc.army.mil/amc/ci/matrix/policy/policy_new.htm

AMC Section 508 Accessibility Guidelines
Found on http://137.80.5.31/section_508/

More information on DoD and DA policy and guidance can be found at: http://www.defenselink.mil/webmasters/ or on the Information Assurance Support Environment located at http://iase.disa.mil/index2.html.

APPENDIX B
Section 508 Web Accessibility Standards Checklist

This page contains a checklist for specific requirements for Web-based information or applications. The Section 508 Web site http://www.section508.gov has a link to the NPRM under Proposed Standards. The Web site of the Center for Information Technology Accommodation (CITA) http://w3.gsa.gov/web/m/old_cita.nsf/RefLib/Concordance#opsys has a link to a document titled: "A Concordance of NPM Requirements and WCAG Checkpoints and Curriculum Examples." The Concordance relates the requirements listed &low to appropriate examples in the W3C Curriculum for Web Content Accessibility.

SEC. 508 STANDARD	PASS	FAIL
(a) A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).	Every image, Java applet, Flash file, video file, audio file, plug-in, etc. has an *alt* description.	A non-text element has no *alt* description.
	Complex graphics (graphs, charts, etc.) are accompanied by detailed text descriptions.	Complex graphics have no alternative text, or the alternative does not fully convey the meaning of the graphic.
	The *alt* descriptions succinctly describe the *purpose* of the objects, without being too verbose (for simple objects) or too vague (for complex objects).	*Alt* descriptions are verbose, vague, misleading, inaccurate or redundant to the context (e.g., the alt text is the same as the text immediately preceding or following it in the document).
	Alt descriptions for images used as links are descriptive of the link destination.	*Alt* descriptions for images used as links are not descriptive of the link destination.
	Decorative graphics with no other function have *empty alt* descriptions (alt= ""), but they never have *missing* alt descriptions.	Purely decorative graphics have *alt* descriptions that say "spacer, "decorative graphic," or other titles that only increase the time that it takes to listen to a page when using a screen reader.

SEC. 508 STANDARD	PASS	FAIL
(b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.	Multimedia files have *synchronized* captions.	Multimedia files do not have captions, or captions, which are not synchronized.
SEC. 508 STANDARD	**PASS**	**FAIL**
(c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.	If color is used to convey important information, an alternative indicator is used, such as an asterisk (*) or other symbol.	The use of a color monitor is required.
	Contrast is good.	Contrast is poor.
SEC. 508 STANDARD	**PASS**	**FAIL**
(d) Documents shall be organized so they are readable without requiring an associated style sheet.	Style sheets may be used for color, indentation and other presentation effects, but the document is still understandable (even if less visually appealing) when the style sheet is turned off.	The document is confusing or information is missing when the style sheet is turned off.
SEC. 508 STANDARD	**PASS**	**FAIL**
(e) Redundant text links shall be provided for each active region of a server-side image map.	Separate text links are provided outside of the server-side image map to access the same content that the image map hot spots access.	The only way to access the links of a server-side image map is through the image map hot spots, which usually means that a mouse is required and that the links are unavailable to assistive technologies.
SEC. 508 STANDARD	**PASS**	**FAIL**
(f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.	Standard HTML client-side image maps are used, and appropriate alt tags are provided for the image as well as the hot spots.	Server-side image maps are used when a client-side image map would suffice.

SEC. 508 STANDARD	PASS	FAIL
(g) Row and column headers shall be identified for data tables.	Data tables have the column and row headers appropriately identified (using the <th> tag)	Data tables have no header rows or columns.
	Tables used strictly for layout purposes do NOT have header rows or columns.	Tables used for layout use the header attribute when there is no true header.
SEC. 508 STANDARD	**PASS**	**FAIL**
(h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.	Table cells are associated with the appropriate headers (e.g., with the *id*, *headers*, *scope* and/or *axis* HTML attributes).	Columns and rows are not associated with column and row headers, or they are associated incorrectly.
SEC. 508 STANDARD	**PASS**	**FAIL**
(i) Frames shall be titled with text that facilitates frame identification and navigation. See Tutorials on "FRAMES".	Each frame is given a title that helps the user understand the frame's purpose.	Frames have no titles, or titles that are not descriptive of the frame's purpose.
SEC. 508 STANDARD	**PASS**	**FAIL**
(j) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	No elements on the page flicker at a rate of 2 to 55 cycles per second, thus reducing the risk of optically induced seizures.	One or more elements on the page flicker at a rate of 2 to 55 cycles per second, increasing the risk of optically induced seizures.

SEC. 508 STANDARD	PASS	FAIL
(k) A text-only page, with equivalent information or functionality, shall be provided to make a Web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.	A text-only version is created only when there is no other way to make the content accessible, or when it offers significant advantages over the "main" version for certain disability types.	A text-only version is provided only as an excuse not to make the "main" version fully accessible.
	The text-only version is up-to-date with the "main" version.	The text-only version is not up-to-date with the "main" version.
	The text-only version provides the functionality equivalent to that of the "main" version.	The text-only version is an unequal, lesser version of the "main" version.
	An alternative is provided for components (e.g., plug-ins, scripts) that are not directly accessible.	No alternative is provided for components that are not directly accessible.
SEC. 508 STANDARD	**PASS**	**FAIL**
(l) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by assistive technology.	Information within the scripts is text-based, or a text alternative is provided within the script itself, in accordance with (a) in these standards.	Scripts include graphics-as-text with no true text alternative.
	All scripts (e.g., JavaScript pop-up menus) are either directly accessible to assistive technologies (keyboard accessibility is a good measure of this), or an alternative method of accessing equivalent functionality is provided (e.g., a standard HTML link).	Scripts only work with a mouse, and there is no keyboard-accessible alternative either within or outside of the script.

SEC. 508 STANDARD	PASS	FAIL
(m) When a Web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with §1194.21(a) through (l).	A link is provided to a disability-accessible page where the plug-in can be downloaded.	No link is provided to a page where the plug-in can be downloaded and/or the download page is not disability-accessible.
	All Java applets, scripts and plug-ins (including Acrobat Portable Document Format (PDF) files and PowerPoint (.PPT) files, etc.) and the content within them are accessible to assistive technologies, or else an alternative means of accessing equivalent content is provided.	Plug-ins, scripts and other elements are used indiscriminately, without alternatives for those who cannot access them.
SEC. 508 STANDARD	**PASS**	**FAIL**
(n) When electronic forms are designed to be completed on-line, the form shall allow people using assistive technology to access the information, field elements, and functionality requiredfor completion and submission of the form, including all directions and cues.	All form controls have text labels adjacent to them.	Form controls have no labels, or the labels are not adjacent to the controls.
	Form elements have labels associated with them in the markup (i.e., the *id* and *for*, HTML elements).	There is no linking of the form element and its label in the HTML.
	Dynamic HTML scripting of the form does not interfere with assistive technologies.	Dynamic HTML scripting makes parts of the form unavailable to assistive technologies.
SEC. 508 STANDARD	**PASS**	**FAIL**
(o) A method shall be provided that permits users to skip repetitive navigation links.	A link is provided to skip over lists of navigational menus or other lengthy lists of links.	There is no way to skip over lists of links.
SEC. 508 STANDARD	**PASS**	**FAIL**
(p) When a timed response is required, the user shall be alerted and given sufficient time to indicate that more time is required.	The user has control over the timing of content changes.	The user is required to react quickly, within limited time restraints.

Section 508 Checklist Notes

Note 1: Until the *longdesc* tag is better supported, it is impractical to use.

Note 2: "Text-only" and "accessible" are NOT synonymous. Text-only sites may help people with certain types of visual disabilities, but are not always helpful to those with cognitive, motor or hearing disabilities.

Note 3: At this time, many elements of Dynamic HTML (client-side scripted HTML, which is usually accomplished with Javascript) cannot be made directly accessible to assistive technologies and keyboards, especially when the onMouseover command is used. If an onMouseover (or similar) element does not contain any important information (e.g., the script causes a button to "glow"), then there is no consequence for accessibility. If this scripted event reveals important information, then a keyboard-accessible alternative is required.

Note 4: When embedded into web pages, few plug-ins are currently directly accessible. Some of them (e.g., RealPlayer) are more accessible as standalone products. It may be better to invoke the whole program rather than embed movies into pages at this point, although this may change in the future.

Note 5: Acrobat Reader 5.0 allows screen readers to access Portable Document Format (PDF) documents. However, not all users have this version installed, and not all PDF documents are text-based (some are scanned in as graphics), which renders them useless to many assistive technologies. It is recommended that an accessible HTML version be made available as an alternative to PDF.

Note 6: PowerPoint files are currently not directly accessible unless the user has a full version of the PowerPoint program on the client computer (and not just the PowerPoint viewer). It is recommended that an accessible HTML version be provided as well.

APPENDIX C
OPSEC Checklist

Operations Security (OPSEC) Checklist For Publicly Accessible Army Websites (v 5.0):			
Name:	Date/Time of Review:		
Organization Reviewed:	Primary IP Address/URL:		
Issue/Concern:	***Yes***	***No***	***Notes/Comments:***
Management Controls (Note: 1): 1. Does the website (WS) contain a clearly defined purpose statement that supports the mission of the DoD Component? 2. Are users of this WS provided with a privacy and security notice prominently displayed or announced on at least the first page of all major sections of each web information service. 3. If applicable does this WS contain a Disclaimer for External Links notice, when a user requests any site outside of the official DoD Web information service (usually the .mil domain)? 4. Is this WS free of commercial sponsorship and advertising? 5. Does each page have webmaster contact information? 6. Does each page show the last modified date? 7. Does each page have a link for an alternative format?			

DEPSECDEF Guidance (Note 2): 1. Operational Information: a. Does the WS contain any information indicating plans or lessons learned which would reveal military operations, exercises or vulnerabilities? b. Does the WS reference any information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program? 2. Personal Information: Does the WS contain personal information in the following categories about U.S. citizens, DOD employees and military personnel: • Social Security Account Numbers? • Dates of Birth? • Home Addresses? • Home Telephone Numbers? • Names, Locations, or any other identifying information about family members of DOD employees or military personnel? 3. Technological Data (Note 3): Does the WS contain any technical data such as: • Weapon Schematics? • Weapon System Vulnerabilities? • Electronic Wire Diagrams? • Frequency Spectrum Data?			

OPSEC Considerations: **"Tip Off Indicators" (Note 4):** Does the WS contain relevant information in the following categories that might reveal an organizations plans and intentions? 1. Administrative: • Personnel Travel (personal and official business) • Attendance at planning conferences • Commercial support contracts 2. Operations, Plans, and Training: • Operational orders and plans • Mission specific training • Exercise and simulations activity • Exercise, deployment or training schedules • Unit relocation/deployment • Inspection results, findings, deficiencies • Unit vulnerabilities or weaknesses 3. Communications: • RF emissions and associated documentation • Changes in activity or communications patterns • Use of Internet and/or e-mail by unit personnel (personal or official business) • Availability of secure communications • Hypertext links with other agencies or units • Family support plans • Bulletin board/messages between soldiers and family members			

4. Logistics/Maintenance: • Supply and equipment orders/deliveries • Transportation plans • Mapping, imagery and special documentation support • Maintenance and logistics requirements • Receipt or installation of special equipment			
Key Word Search: Using the following "key words" conduct a search using the search tool. As a result of this search conduct a random screen of any documents found: • Deployment Schedules • Exercise Plans • Contingency Plans • Training Schedules • Inspection results, findings, deficiencies • Biographies • Family Support Activities • Phone Directories, Lists			
Coding: The following will be tested for: • Broken Links • Broken Code • Clean HTML, JavaScript, XML Code *Note: code can be tested and cleaned up using the HTML validator and other code validation tools provided by W3 Consortium at* http://www.w3.org/			

NOTES PAGE

Note 1: Management Controls are contained in the policy published by the Office of the Secretary of Defense, titled: Establishing and Maintaining A Publicly Accessible Department of Defense Web Information Service, 9 January 1998.

Note 2: These elements were pulled directly from the DEPSECDEF memo, Information Vulnerability and the World Wide Web, dated, 24 Sept 98.

Note 3: Technical data creates a unique challenge to the OPSEC posture of an organization and to National Security as a whole. Certain technical data, when compiled with other unclassified information, may reveal an additional association or relationship that meets the standards for classification under Section 1.8 (e) E.O. 12958.

Note 4: "Tip-off" indicators are pulled directly from AR 530-1, Operations Security (OPSEC) regulation, dated 3 Mar 95. Tip-off indicators highlight information that otherwise might pass unnoticed. These are most significant when they warn an adversary of impending activity. This allows him to pay closer attention and to task additional collection assets.

By necessity this list is generic in nature. There are many other indictors possible for the wide range of military operations and activities. While this list is rather large - when placed in the context of a command's ***pre-established*** critical information, this list may then be applied with a greater level of accuracy. This checklist is not a panacea for complete organizational OPSEC program. If an organization has not invested the effort to analyze its own critical information, then this list may only tend to exacerbate the problem.

Within the context of information assurance, the World Wide Web should not be treated any differently from any other potential vulnerability. Security of information on publicly accessible Websites must be viewed in the context of an organization's overall OPSEC posture.